Navigating the data breach minefield: strategies

Bridget Treacy, Partner at Hunton & Williams, provides invaluable guidance for organisations in limiting their damage for when a data disaster strikes

Data is the lifeblood of our global economy, and the threat of interruption to corporate IT networks has never been greater. Information management and information security are key processes for all organisations. Across Europe, data security breaches are now board level issues, not least because of the negative publicity they generate and the cost of addressing them. The data protection regulator in the UK, the Information Commissioner ('Commissioner'), disclosed recently that almost four hundred data breaches were reported to his office during the last twelve months. This despite there being, strictly speaking, no compulsory data breach notification law in the UK. Have we now reached the position in the UK where we have a de facto data breach law? Many UK organisations think so, and are looking to the experience of US based organisations of data breach, to prepare for what many regard as a business inevitability.

Origin of data breach laws

'Data breach' is a generic term, applied to an array of instances in which the security or integrity of data is compromised, whether deliberately or not. In the US, it is now the norm to notify data breaches, but the triggers for notification, and the recipients of any notification, will vary on a state by state basis. The US data breach laws had their genesis in the California Computer Security Breach Notification Act (S.B. 1386), which came into effect on 1st July 2003. Over time, the Californian requirement to notify individuals of data breach incidents has come to include all affected persons, whether they reside in California or not. More than 40 individual states in the US have enacted data breach laws.

There has been much analysis of the effectiveness of US data breach laws. Such analysis has focussed in particular on whether the notification requirement itself contributes significantly to the reduction of identity theft and other losses which may result from a data breach incident. It is difficult to draw the clear conclusion that data breach laws reduce identity theft. However, what is clear is that the existence of the laws and consequences (including the cost of dealing with a breach incident, and the fear of the attendant negative publicity), act as an incentive to organisations to ensure that data are safeguarded. Further, with breaches regarded as an inevitability, there is an increased focus in the US on ensuring adequate preparations are made for dealing with breach incidents.

In the EU, there is currently no general legal requirement for organisations to notify their data breaches, either to regulators or to the individuals whose data have been compromised. However, that position is changing. The national laws of some EU jurisdictions now include obligations to notify data breaches, and local practice or local regulators may also dictate that breaches are notified. Further, the e-Privacy Directive, which is currently under review, is certain to contain a breach notification obligation.

UK data breach laws

Whilst the UK may not have data breach laws in the US sense, developments in both law and practice since the infamous 'HMRC' data breach in 2007 (see Volume 8, Issue 7, pages 7 — 8 of *Privacy & Data Protection*) mean that, for practical purposes, UK organisations are subject to a breach notification regime. There are three key elements to this regime:

i) the security principle under the Data Protection Act 1998 ('DPA');

ii) fines for serious breaches of the DPA; and

iii) the Commissioner's expectation that serious breaches will be notified.

Security Principle

The Seventh Data Protection Principle ('Security Principle') in the DPA requires data controllers to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data. Further, it requires that appropriate measures are taken to prevent accidental loss or destruction of, or damage to, personal data.

It is difficult to imagine a data breach incident which would fall outside the scope of this provision. Recent high

(Continued on page 12)

(Continued from page 11)
profile breaches in the UK, which have been the subject of enforcement proceedings by the Commissioner, have all involved a breach of the Security Principle. For example:

- when various high street banks carelessly disposed of personal data in rubbish bins;
- when the Home Office and one of its subcontractors, PA Consulting, lost the personal data relating to convicted criminals. That data was downloaded from a Home Office database onto an unencrypted memory stick by a PA Consulting employee in 2008;
- when HMRC lost the entire UK child benefits database. A junior employee downloaded the data onto two unencrypted CDs which were lost in the post in 2007; and
- when Marks & Spencer pension consultants suffered the theft of an unencrypted laptop containing employee pension details.

Fines for serious breaches of the DPA

A new section 55A of the DPA, widely expected to come into effect during 2009, empowers the Commissioner to impose fines on data controllers where there is a serious breach of the DPA. The contravention must be likely to cause substantial harm or distress, and the data controller must have knowingly or recklessly failed to prevent the breach. Once this section is in force, serious security breaches are likely to attract fines. The fines will be calculated as a percentage of an organisation's turnover.

The inclusion of a concept of 'recklessness' into section 55A means that organisations will be penalised for their failure to take steps even where they were unaware that the breach would be likely to cause substantial damage. Organisations will be unable to hide behind protestations of ignorance. They will be expected to demonstrate that they have in place appropriate data protection policies and procedures.

"Communications must be carefully drafted. They need to be informative, and must be written in plain English. They must not include any details of the compromised data"

Notification of breach

Notwithstanding the absence of a legal requirement, the Commissioner has expected data controllers to notify serious data breaches to the Information Commissioner's Office ('ICO') for some time now. The Commissioner's guidance on data breach indicates that the decision to notify must have regard to the volume and sensitivity of the data which has been compromised, and to the likelihood of harm to individuals. The ICO then works with organisations to determine whether notification to individuals would serve any useful purpose. The Commissioner has indicated in the past that he is mindul of the risks of 'notification fatigue', i.e. where individuals receive multiple notices on a regular basis, and take little notice of them.

The development of a European data breach law

Calls for an EU level data breach law are intensifying, in part as a consequence of recent high profile breaches, particularly in Germany.

The e-Privacy Directive, which governs the processing of data and the protection of privacy in the electronic communications sector, is being reviewed as part of a wider review of access to communications services. One of the proposed amendments to the e-Privacy Directive is a new requirement for providers of publicly available communication services to notify security beaches. There has been lengthy debate within the European Commission, European Parliament and European Council as to whether the notification obligation will require notification to regulators, or to individuals, or both. There is also continuing debate as to whether the obligation will apply to providers of information society services (e.g. online retailers, banks and the like), or only to communications services providers (e.g. ISPs). Further, there is currently uncertainty as to whether the service provider itself or the national data protection regulator will determine whether a breach should be notified.

Recently, the Article 29 Working Party published a further Opinion (1/2009) on the proposed amendments to the e-Privacy Directive (their third set of comments on the issue). The Opinion urges that service providers notify breaches to regulators, but determine themselves whether the breach should be notified to individuals. In addition, the Working Party proposes that regulators may take the decision themselves to disclose a breach publicly. The Working Party recommends that clear criteria are established to assess the impact of adverse effects caused by any breach, and that national regulators have the power to impose financial penalties where a service provider fails to report a breach.

Despite the discussions to date, the views of the European Commission, European Parliament, and European Council still differ on the following outstanding issues:

- the scope of the notification obligation (i.e. information society services or communications services providers);
- the entity which determines whether to notify individuals (i.e. the national regulator or service provider);
- the types of breaches to be notified (i.e. all breaches or only serious breaches); and

- the persons who may be notified (subscribers or individuals affected).

Managing the inevitable

Although the underlying legislative provisions are in a state of flux, data breaches continue to occur and must be managed, irrespective of whether or not there is a formal requirement to notify regulators or individuals. The existence of globally networked information management systems means that a data breach in one jurisdiction can have serious repercussions in another jurisdiction. Many breaches have an international element requiring a co-ordinated approach in containing them. As a result, organisations are increasingly drawing on the experience of US organisations for guidance on how best to deal with breaches.

What, where and who

The crucial first step in managing data breaches is to determine what information is affected by the breach, where the information is processed, and which entity is responsible for it.

This investigation requires an awareness of the fact that even a basic concept, such as the definition of 'personal data', may have different meanings in different jurisdictions. In the US, notification obligations may be triggered where specific combinations of data have been compromised, or where data held in a specific format are compromised. In Europe, the focus is on the processing of 'personal data', a broadly defined concept.

Whether or not any compromised information was encrypted, can be highly relevant. In the US, encryption creates a safe harbor under data breach notification laws. Data breach laws in Europe are still being developed, but in the UK the use of encryption technologies will be taken into account by the Commissioner in assessing whether individuals should be notified of the breach, and in determining what enforcement action may follow. Many of the data breaches which have created news headlines in the UK have concerned unencrypted laptops and USB drives.

It is important to consider where the compromised data have been processed, and by whom. In the EU, legal responsibility for personal data rests with the data controller, irrespective of whether the data have been passed to a third party for processing in a foreign jurisdiction. This issue is important in an outsourcing context, or where data are processed in a group context, or using distributed or cloud computing models. In such cases, it is crucial to ensure that the entity with responsibility for the personal data i.e. the data controller is informed promptly of any data breaches, and that other parties involved in any data processing operations co-operate fully in investigating the event as promptly as possible. Contractual arrangements may play a crucial role in ensuring that the data controller is able to take charge and act swiftly.

The answers to many of these initial questions will require investigation and analysis, frequently with the involvement of forensic investigators who can assist in preserving potential evidence for subsequent litigation. Data breaches must be made known to the right team, and not treated as an IT problem. The effects of a data breach incident will be felt far beyond the remit of the IT team.

A number of internal stakeholders within an organisation will need to be informed of any data breaches. However, considerable care should be taken to ensure that the organisation's internal investigation is protected, to the greatest extent possible, by legal professional privilege. Engaging the organisation's general counsel, or external counsel, from the outset can assist in preserving legal professional or litigation privilege.

Informing stakeholders

The array of potential stakeholders who may need to be involved in a data breach incident is wider than many realise. To assist in determining the cause and scope of a breach, the board or senior executives will need to be informed (in addition to IT professionals). Senior executives will want to know that the source of the incident has been identified and secured. They will also want to know whether the organisation has complied with relevant standards (such as Payment Card Industry Standards), and its own information security policy.

Where criminal activity is suspected, the organisation will need to notify to and work with relevant law enforcement agencies. Further, if the organisation operates in a regulated sector, it may be necessary to notify industry regulators, e.g. the Financial Services Authority. If a significant volume of data are compromised, the nature of the compromised information is sensitive, or there is a real likelihood of harm to individuals, then the Commissioner may need to be notified. This can be done via email, and should include the following information:

- the type of data and number of records compromised;
- the circumstances of the loss;
- the action taken to minimise or mitigate effects on the individuals involved;
- details of how the breach is being investigated;
- whether any other regulatory body has been informed, and details of their response; and
- details of any remedial action taken to prevent future occurrence.

Organisations may have contractual relationships which oblige them to notify other parties of data breaches. For example, credit or payment card issuers may need to be notified, and it may also be prudent to notify the organisation's insurers.

Informing individuals

The individuals whose data have been compromised will be a key focus of any notification activity, particularly if there is the possibility of individuals being able to take positive steps to reduce the likelihood of identity theft or other harm. Communications designed to inform individuals that their data may be compromised

(Continued on page 14)

(Continued from page 13)
must be carefully drafted. They need to be informative, and must be written in plain English. The notification should describe the breach and, where appropriate, organisations should accept responsibility for events rather than shifting the blame elsewhere. The organisation should also explain what it is doing to help those affected by the breach (including a reference to credit monitoring if appropriate), and state clearly what steps individuals are encouraged to take (such as checking bank statements, changing passwords, etc). These communications must not include any details of the compromised data.

Notification communications are read by many people, including regulators, claimants' lawyers, the media and, of course, the individuals whose data have been compromised. Accordingly, they must be drafted with care and usually by a group of people including lawyers, corporate communications experts and senior executives.

Learning from the US experience

US companies consider data breaches as an inevitability. Consequently they are proactive in creating data breach response plans. The starting point for any such plan is to undertake a risk assessment of the organisation's systems and security, and determine which systems — if breached — present the most significant risks to the organisation. Key systems must be monitored and assessed regularly, and a breach response plan developed. Also, employees should be aware of the existence of the plan, and familiar with other security breach guidance. Organisations can save valuable time following a data breach if a breach response team, familiar with the breach response plan, is appointed in advance.

Conclusion

Managing data breaches is a new challenge for many organisations in Europe. The experience of US organisations suggest that advance preparation is key to dealing successfully with these incidents. Once a breach occurs, events move at a lightening pace, and organisations with little idea of what personal data they process, let alone where or how the data are processed, will struggle to stay on top of developments. Under the full glare of the media spotlight, mistakes are easily made, and may destroy attempts to contain these incidents. Recent US and EU experience suggests that data breaches are an inevitability, and that organisations which survive data breaches relatively unscathed are those which prepare.

Bridget Treacy
Hunton & Williams
btreacy@huntonwilliams.com